BAB I
PENDAHULUAN

1.1. Latar Belakang

Penerapan teknologi informasi sekarang banyak digunakan di berbagai bidang, terutama pada bidang kesehatan. Pentingnya pengelolaan data kesehatan diperlukan suatu rancangan kerangka kerja konseptual untuk terlaksananya *Health Information Technology* (HIT) [1]. Meningkatnya penggunaan teknologi pada bidang kesehatan membutuhkan peningkatan kualitas data dan produk sistem informasi.

Simkesmas (Sistem Informasi Manajemen Kesehatan Masyarakat) merupakan sistem informasi penunjang layanan kesehatan berbasis *online* pada Puskesmas yang bertujuan untuk mempermudah administrasi dan pelayanan puskesmas. Seiring dengan berjalannya waktu pengembangan Simkesmas selain dilakukan perbaikan dan penambahan fitur, saat ini sudah dirancang suatu konsep sistem "Jejaring" yang menjaring layanan kesehatan yang berada pada cakupan Puskesmas. Sistem tersebut direncanakan berupa *mobile application*, *desktop application* dan *web based* yang terpisah dari Simkesmas.

Data yang diperlukan untuk "Jejaring" seperti data pasien, data diagnosa dan lain sebagainya, akan diambilkan dari *database* Puskesmas terkait. *Web service* untuk pertukaran data Simkesmas sangat diperlukan agar dapat berkomunikasi dengan aplikasi "Jejaring". Dikarenakan Simkesmas memuat data kesehatan yang bersifat rahasia dan sensitif, maka diperlukan pengamanan ekstra dalam autentikasi dan manipulasi data pada *web service* berupa penggunaan *token* yang terdapat *digital signature*-nya.

Web service sendiri merupakan suatu sistem perangkat lunak yang dibuat untuk memudahkan interaksi antar sistem di atas jaringan dan terbuka untuk semua platform [2]. *Web service* digunakan untuk menyediakan informasi atau data untuk sistem lain, sehingga kedua sistem tersebut bisa saling berinteraksi melalui layanan-layanan yang telah disediakan.

Untuk alasan keamanan *web service* dikembangkan menggunakan protokol HTTPS (*Hypertext Transfer Protocol Secure*) yang merupakan kombinasi merupakan HTTP dan protokol SSL/TLS. HTTP m1erupakan protokol yang kurang

terjamin keamanannya. Ketika *client* berkomunikasi pada jaringan yang menggunakan protokol HTTP, maka orang lain dapat melakukan *eavesdrop* komunikasi antara *client* dan *server* [3].

Pada penelitian yang telah dilakukan oleh Penidas Fiodinggo Tanaem, Danny Manongga dan Ade Iriani (2016) tentang *RESTful web service* untuk sistem pencatatan transaksi perusahaan pemasaran perhiasan. Menjelaskan bahwa perusahan tersebut mempunyai beberapa masalah pengelolaan data yang disebabkan oleh masing-masing unit di perusahaan tersebut berbeda [4]. Maka diterapkan *web service* untuk mengatasi masalah tersebut. *Web service* tersebut diimplementasikan digital signature dengan menggunakan algoritma HMAC untuk melengkapi aspek keamanan. Hasil pengujian penelitian tersebut algoritma HMAC dapat memberikan keamanan sebagai *digital signature*. Akan tetapi algoritma HMAC tidak memenuhi aspek *non-repudiation*, yaitu aspek yang menjamin seseorang tidak dapat menyangkal telah melakukan suatu transaksi.

Pada penelitian Andy Triwinarko *mengenai Elliptic Curve Digital Signature Algorithm* (ECDSA) menyatakan bahwa ECDSA dengan panjang kunci 160 bit mempunyai tingkat keamanan yang relatif sama dengan RSA dengan panjang kunci 1024 bit [5]. ECDSA mempunyai keunggulan berupa ukuran panjang kunci yang lebih kecil dibanding RSA dan memiliki tingkat keamanan yang relatif sama, sehingga algoritma ECDSA cocok untuk digunakan pada sistem yang mempunyai sumber daya terbatas. Dan algoritma ECDSA maupun RSA sama-sama memenuhi aspek *non-repudiation* untuk *digital signature*.

Pada penelitian yang dilakukan Pualam Sendi, Idris Winarno, dan Nur Rosyid (2010) tentang impelementasi algoritma ECDSA untuk verifikasi keaslian pesan *email*. Menjelaskan bahwa algoritma ECDSA yang telah diimplementasikan pada aplikasi *email client* dapat memverifikasi keaslian pesan yang diterima, dengan catatan penerima *email* memiliki kunci *public* [6].

Merujuk pada latar belakang yang telah dijabarkan, pada penelitian ini akan dilakukan implementasi *non-repudiation web service* menggunakan algoritma ECDSA. Adanya implementasi algoritma ECDSA diharapkan selain memberikan keamanan pada *web service* juga memberikan performa yang bagus dan memberi kontribusi terhadap penelitian-penelitian sebelumnya.

1.2. Rumusan Masalah

Adapun rumusan masalah dalam penelitian ini adalah sebagai berikut :

a. Bagaimana mengimplementasikan algoritma ECDSA pada web service untuk memenuhi aspek keamanan *non-repudiation*?
b. Bagaimana mengukur performansi *signing* dan *verifying* algoritma ECDSA dan RSA dari hasil implementasi yang telah dilakukan?
c. Bagaimana mengukur performansi *generate token* algoritma ECDSA, HMAC dan RSA pada *token* JWT?

1.3. Batasan Masalah

Terdapat beberapa batasan masalah yang diangkat sebagai parameter pengerjaan tugas akhir ini diantaranya adalah sebagai berikut:

a. *Backend web service* dikembangkan pada *framework* Lumen, sedangkan *Frontend web service* dikembangkan pada *framework* Laravel
b. Jumlah *database server* yang digunakan untuk *web service* berjumlah 7
c. *Web service* menggunakan protocol HTTPS
d. Implementasi algoritma ECDSA dan RSA menggunakan JWT (*Json Web Token*)
e. Uji coba dilakukan dengan menggunakan *tool Postman*, JWT Debugger dan *John The Ripper*.

1.4. Tujuan Penelitian

Tujuan dari penelitian ini adalah merancang *web service multi database* dan mengimplementasikan algoritma ECDSA sebagai *digital signature* untuk memenuhi aspek keamanan *non-repudiation*.

1.5. Metodologi

Dalam penyusunan tugas akhir ini, metodologi penelitian yang digunakan adalah:

1.5.1. Studi Pustaka

Studi pustaka merupakan tahapan untuk memahami konsep dari pembangunan sistem yaitu mengenai algoritma ECDSA dan *framework* Lumen dan Laravel. Pemahaman konsep didapatkan dari berbagai jurnal, karya tulis ilmiah dan buku yang berhubungan dengan algoritma ECDSA dan *framework* Lumen dan Laravel.

1.5.2. Analisis Kebutuhan

Pada tahap ini penulis melakukan analisis terkait beberapa kebutuhan baik kebutuhan fungsional maupun non-fungsional untuk menunjang sistem *web service*.

1.5.3. Desain Sistem

Pembuatan arsitektur sistem, gambaran sistem dan rancangan desain antarmuka akan dibuat pada tahap ini dengan didasarkan pada analisis kebutuhan yang sudah dilakukan untuk mendukung proses implementasi.

1.5.4. Implementasi Sistem

Pada tahap ini dilakukan pembangunan aplikasi *web* service baik *frontend* untuk *admin* dan backend. Implementasi dilakukan berdasarkan hasil analisis kebutuhan dan desain sistem yang sudah dilakukan.

1.5.5. Pengujian dan Evaluasi

Uji coba terhadap aplikasi yang sudah dibangun dilakukan pada tahap ini. Skenario pengujian dibuat dan dilakukan untuk diketahui hasilnya.

1.5.6. Penyusunan Laporan

Tahap ini merupakan tahap akhir setelah menyelesaikan tahap-tahap sebelumnya. Laporan yang ditulis merupakan seluruh hasil analisis dan pengujian serta kesimpulan dari hasil penelitian yang sudah dilakukan.

1.6. Sistematika Penulisan

Sistematika penulisan laporan penelitian ini disusun menjadi beberapa bab sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi pendahuluan yang menjelaskan latar belakang, rumusan masalah, tujuan penelitian, batasan permasalahan, metodologi, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini berisi landasan teori sebagai parameter rujukan untuk dilaksanakannya penelitian ini. Adapun pengkajian materi tersebut adalah kajian tentang *web service, Elliptic Curve Digital Signature Algorithm, framework* Lumen dan Laravel, dan beberapa kajian pendukung lainnya.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini berisi analisis dan perancangan aplikasi yang dibangun mulai dari analisis masalah, kebutuhan, hingga desain *user interface.* Hal ini dilakukan untuk memberikan gambaran jelas pada saat implementasi *coding* dilakukan

BAB IV IMPLEMENTASI DAN PENGUJIAN

Bab ini berisi tentang implementasi pengembangan aplikasi berdasarkan analisis dan perancangan sistem yang sudah dilakukan pada BAB III, yang berlanjut dengan pengujian terhadap fungsionalitas aplikasi tersebut.

BAB V PENUTUP

Bab ini memuat tentang kesimpulan dan saran yang diperoleh dari hasil penelitian untuk pengembangan maupun referensi di masa yang akan datang.